(2)

Department of Defense
DIRECTIVE

December 9, 1996
Number S-3600.1

ASD (C3I)

SUBJECT: Information Operations (IO) (U)

References: (a) DoD Directive TS-3600.1, "Information Warfare (U)," December 21, 1992 (hereby canceled).
(b) DoD Instruction S-3600.2, "Information Warfare Security Classification Guidance (U)," February 6, 1996

A. REISSUANCE AND PURPOSE

(U) This Directive reissues reference (a) to update IO and Information Warfare (IW) policy, definition, and responsibilities within the Department of Defense.

B. APPLICABILITY

(U) This Directive applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components").

C. DEFINITIONS

(U) Terms used in this Directive are defined in the enclosure.

D. POLICY

1. (U) The Department of Defense must be prepared for missions from peace to war to include military operations other than war (MOOTW), such as peace-keeping and humanitarian operations, opposed by a wide range of adversaries including State and non-State actors. To meet this challenge, DoD activities shall be organized, trained, equipped, and supported to plan and execute IO. The goal of IO is to secure peacetime national security objectives, deter

~~Classified by: Emmett Paige, Jr.~~
~~ASD(C3I)~~
~~Reason: 1.5 (a) and (c)~~
~~Declassify on: December 31, 2007~~

conflict, protect DoD information and information systems, and to shape the information environment. If deterrence fails, IO seek to achieve U.S. information superiority to attain specific objectives against potential adversaries in time of crisis and/or conflict. The goal of IO is to promote freedom of action for U.S. forces while hindering adversary efforts.

a. (U) IO exploit the opportunities and vulnerabilities inherent in dependence on information to support military activities. IO include actions taken in the information environment by the Department of Defense to achieve specific objectives over any potential adversary. IO are conducted across the full range of military operations. The focus of IO is on decisionmaking and information-dependent systems, including weapons, infrastructure, command and control, computer, and associated network systems. These involve not only hardware and software but also associated personnel.

b. (U) IO impact, and are impacted by, military activities on the land, at sea, in the air, and in space in the areas that influence information and information systems. This policy establishes the requirement that IO activities support and are supported by other military activities and are considered in all appropriate contexts.

(b)(1)

d. (U) Across the full range of military operations, IO are controlled through an approval process appropriate to the sensitivity of the specific activity in question. Certain IO activities inherent and granted to the Secretary of Defense, including some SIO, may require coordination outside of the Department of Defense. Such coordination will be conducted when customary or deemed necessary and approved during the operations plan review and approval process.

2. (U) IO considerations shall be carefully evaluated when developing policy, defining and validating requirements, conducting research and development, acquiring systems, and planning and executing operations.

3. (U) Public Affairs during IO planning must not focus on directing or manipulating public actions or opinions but rather seek a timely flow of information to both external and internal audiences. Coordination of PA and IO plans is required to ensure that PA initiatives support the commander's overall objectives. PA and IO efforts will be integrated consistent with policy or statutory limitation.

4. (U) Civil Affairs activities are important to IO because of their ability to interface with key organizations and individuals in the information environment. Civil Affairs can support and assist IO objectives by coordinating with, influencing, developing, or controlling indigenous infrastructures in foreign operational areas.

5. (U) Intelligence must be readily accessible, timely, accurate and sufficiently detailed to support an array of DoD IO requirements, to include research, development and acquisition and operational support. Detailed intelligence on the information systems and the IO doctrine likely to be employed by a wide range of adversaries must be provided.

(b)(1)

7. (U) To achieve the fullest possible integration of IO, the DoD Components shall share tactics, techniques, procedures and technologies to the maximum extent practicable.

8. (U) The Department shall vigorously pursue IA activities to prevent adversarial effects on our information and information systems. The DoD Components shall work toward a multi-layered information systems defense that incorporates protection, detection, reaction, and reconstitution using risk-based management principles. DoD information systems critical to the transmission and use of minimum-essential information for command and control of forces shall be designed, employed, and exercised in a manner that minimizes or prevents exploitation, degradation, or denial of service from a multiple variety of attacks to include CNA. Command and control of forces shall be planned and exercised to ensure critical information is adequately protected from adversary IW effects and U.S. forces can operate successfully in degraded information and communications environments.

9. (U) To prepare for crisis and conflict, the Department of Defense shall be organized, trained, equipped, and supported to plan and execute IW against specific adversaries. IW is an integral part of modern military operations, thus enhancing the capability of U.S. Armed Forces to win quickly and decisively, with minimum losses and collateral effects.

10. (U) Sufficient training, including realistic exercises that simulate peacetime and wartime stresses, shall be conducted to ensure that commanders of U.S. Armed Forces are well-informed about trade-offs among affecting, exploiting, and destroying adversary information systems, as well as the varying capabilities and vulnerabilities of DoD information systems. The training shall also include an understanding of the interrelationship between the two. Also, the DoD

Components shall create realistic IO environments for planning, training, and acquisition purposes to include models and simulations.

E. RESPONSIBILITIES

1. (U) The Deputy Secretary of Defense shall:

a. (U) Oversee the DoD role in the inter-agency process concerning IO.

b. (U) Review and obtain Secretary of Defense approval for SIO.

c. (U) At the direction of the Secretary of Defense, assist in the exercise of National Command Authorities (NCA) control over SIO.

2. (U) The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence shall:

a. (U) Serve as the principal staff assistant and advisor to the Secretary of Defense and Deputy Secretary of Defense for DoD IO.

b. (U) Act as the central point of contact for the Department of Defense on IO, consistent with other identified responsibilities.

c. (U) Review DoD IO plans, programs, and requirements to monitor and evaluate program responsiveness to validated requirements.

d. (U) Deconflict DoD IO programs.

e. (U) Coordinate and deconflict dual use techniques, procedures and technologies.

f. (U) Exercise oversight for centralized planning and coordination and decentralized execution of IO matters, to include broad strategy, program and budget review, technology development, security guidance (see DoD Instruction S-3600.2, reference(b)), and education and training.

g. (U) Develop IO assessment methodologies and metrics.

h. (U) Oversee applicable training and career development policy to ensure that trained personnel are available to support and participate in IO.

i. (U) Coordinate with the Under Secretary of Defense for Acquisition and Technology (USD(A&T)) when IO matters pertain to USD(A&T) responsibilities, EW, and Space Control.

j. (U) Coordinate with the Under Secretary of Defense for Policy (USD(P)) when IO matters pertain to USD(P) responsibilities, psychological operations, and deception.

k. (U) Working with the the Secretaries of the Military Departments, Defense Intelligence Agency (DIA) and the Defense Information Systems Agency (DISA), through the Joint Staff, assist Combatant Commands with the development of command C4ISR architecture planning and programs that fully integrate IO support requirements.

l. (U) Require the Director, DISA, to:

(1) (U) Serve as the DoD focal point to oversee the application of information protection for the Defense Information Infrastructure.

(2) (U) Plan, develop, coordinate, and support the automated information systems (including the command, control, communications, and computer systems) that serve the needs of the NCA under all conditions of peace and war. Ensure that such systems respond to and incorporate IA requirements.

m. (U) Require the Director, DIA, to:

(1) (U) Manage Defense intelligence community production to support the full range of DoD IO.

(2) (U) Oversee DoD requirements, and serve as the Defense intelligence community focal point, for the development, management, and maintenance of information systems and databases that facilitate timely collection, processing, and dissemination of all-source, finished intelligence for DoD IO.

(3) (U) As DoD human intelligence (HUMINT) manager, provide oversight, guidance, and direction to the Defense HUMINT service, consistent with DoD IO objectives.

(4) (U) Coordinate with the DoD Components to share IO techniques and related intelligence.

(5) (U) Serve as the focal point for DoD IW indications and warning activities. Provide the Chairman of the Joint Chiefs of Staff and the Combatant Commands with the timely intelligence required for effective IW target selection and post-strike analysis.

3. (U) The Under Secretary of Defense for Acquisition and Technology shall:

a. (U) Develop policy, in coordination with the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD(C3I)), when IO matters pertain to USD(A&T) responsibilities, EW, and Space Control.

b. (U) Review and approve information systems technology and tactical IO system acquisition programs; ensure that adequate science and technology programs exist to support IO systems; provide oversight for the development and acquisition of systems that support IO; and ensure protection, detection, and reaction measures are considered during systems development.

4. (U) The Under Secretary of Defense for Policy shall:

a. (U) Develop policy, in coordination with the ASD(C3I), when IO matters pertain to USD(P) responsibilities, psychological operations, and deception.

b. (U) Review IO and IW plans to ensure integration of DoD plans with overall national security objectives.

c. (U) Lead inter-agency discussions on IO policy.

d. (U) Coordinate the inter-agency approval process for applicable SIO.

5. (U) The General Counsel of the Department of Defense shall review all proposed SIO and provide legal advice and assistance to the Secretary of Defense and the Deputy Secretary of Defense and all other responsible Department of Defense officials.

6. (U) The Secretaries of the Military Departments shall:

a. (U) Develop IO doctrine and tactics; and organize, train, and equip to ensure that IO become effective elements of, and integral to, U.S. military capabilities.

b. (U) Define IO requirements. Program and budget resources for validated requirements. Develop, modify or acquire systems in response to validated service requirements. Ensure systems meet DoD standards and joint interoperability requirements.

c. (U) Ensure that command and control, and sustainment of forces, shall be planned so that critical information is identified and adequately protected from adversary effects.

d. (U) Review related Service classified programs annually for applicability to IO and advise the ASD(C3I) of results.

(b)(1)

7. (U) The Chairman of the Joint Chiefs of Staff shall:

a. (U) Serve as the principal military advisor to the Secretary of Defense on IO.

b. (U) Validate IO requirements through the Joint Requirements Oversight Council.

c. (U) Establish doctrine to facilitate the integration of IO concepts into joint operations.

d. (U) Ensure plans and operations include and are consistent with IO policy, strategy, and doctrine.

e. (U) Coordinate with the commanders of the Combatant Commands to ensure effective planning and execution of IO.

f. (U) Ensure that exercises routinely test and refine IO capabilities, including the application of realistic wartime stress to information systems.

g. (U) Ensure joint command and control is sufficiently robust to support continued operations should U.S. information systems be degraded.

h. (U) Incorporate IO into the joint military education curricula.

8. (U) The Director, National Security Agency, shall:

a. (U) Provide Signals Intelligence and technology assessments in support of IO planning and operations. In addition, provide Intelligence Gain/Loss Assessments (IG/LA) to support proposed IO.

b. (U) In conjunction with appropriate Agencies, assess and provide information systems security threat and vulnerability information to support IO requirements.

c. (U) As the National Manager for National Security Telecommunications and Information Systems Security, develop information security technology and techniques required to protect information and information systems against adversary effects. Assist in their implementation by conducting evaluations of their effectiveness.

(b)(1)

e. (U) Coordinate IO support activities with Secretaries of the Military Departments, Chairman of the Joint Chiefs of Staff, and the Heads of the DoD Components.

9. (U) The Heads of the DoD Components shall assign responsibilities and establish procedures within their organizations to implement the policies in section D., above. The Component heads shall apprise the Director, NSA, of developmental efforts consistent with subsection E.8., above.

F. EFFECTIVE DATE

(U) This Directive is effective immediately.

John P. White
Deputy Secretary of Defense

Enclosure
Definitions

DEFINITIONS

1. (U) Computer Network Attack (CNA). Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.

(b)(1)

3. (U) Information. Facts, data, or instructions in any medium or form.

4. (U) Information Assurance (IA). IO that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

5. (U) Information Environment. The aggregate of individuals, organizations, or systems that collect, process or disseminate information, also included is the information itself.

6. (U) Information Operations (IO). Actions taken to affect adversary information and information systems while defending one's own information, and information systems.

7. (U) Information Superiority. The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

8. (U) Information System. The entire infrastructure, organization, personnel and components that collect, process, store, transmit, display, disseminate and act on information.

9. (U) Information Warfare (IW). IO conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.

10. (U) Special Information Operations (SIO). IO that by their sensitive nature, due to their potential effect or impact, security requirements, or risk to the national security of the U.S., require a special review and approval process.